Threat Modeling

Michael Howard
mikehow@microsoft.com
Senior Program Manager
Secure Windows Initiative
Microsoft Corp.

Threat Modeling

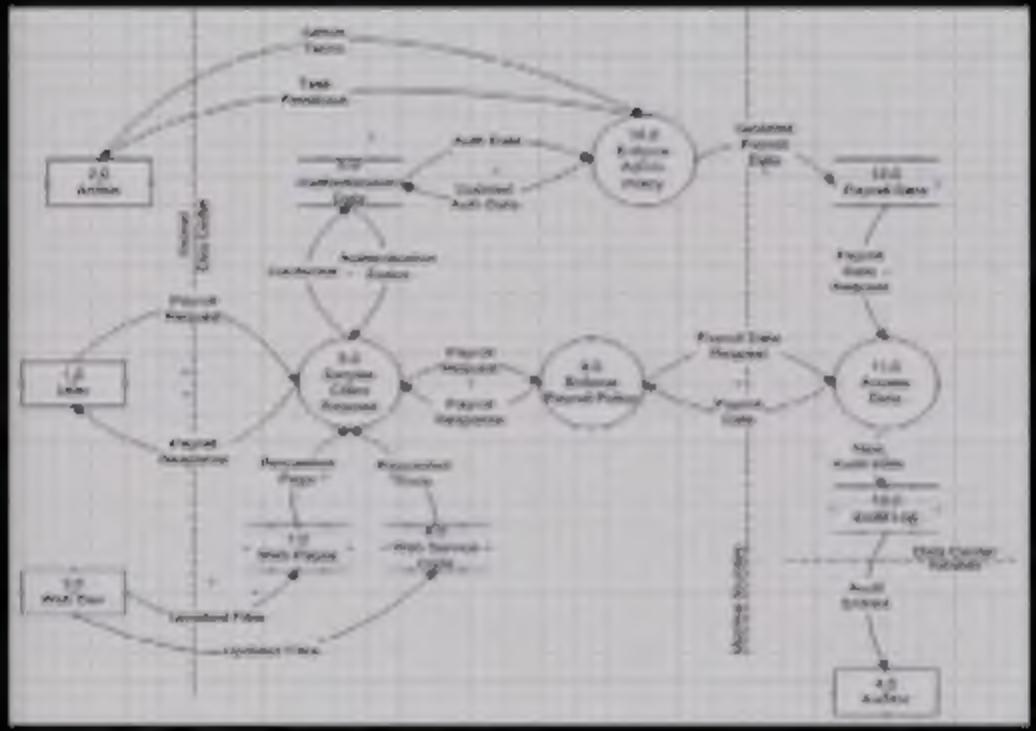
Michael Howard
mikehow@microsoft.com
Senior Program Manager
Secure Windows Initiative
Microsoft Corp.

Threat Analysis

- You cannot build secure applications unless you understand threats
  - Adding security features does not mean you have secure software
  - "We use SSL!"
- Find issues before the code is created
- Find different bugs than code review and testing
  - Implementation bugs vs higher-level design issues
- Approx 50% of issues come from threat models

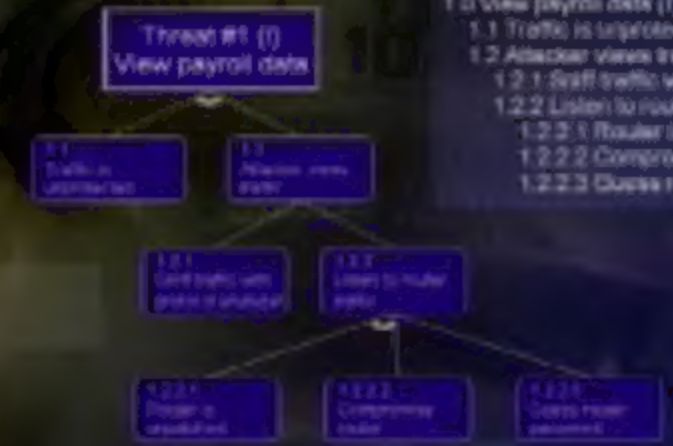
Threat Modeling Process

- Create model of app (DFD, UML etc)
  - Build a list of assets that require protection
- Categorize threats to each attack target node with STRIDE
  - Spoofing, Tampering, Repudiation, Info Disclosure, Denial of Service, Elevation of Privilege
- Build threat tree for each threat
  - Derived from hardware fault trees
- Rank threats by risk
  - Risk = Potential * Damage
  - DREAD: Damage potential, Reproducibility, Exploitability, Affected Users, Discoverability



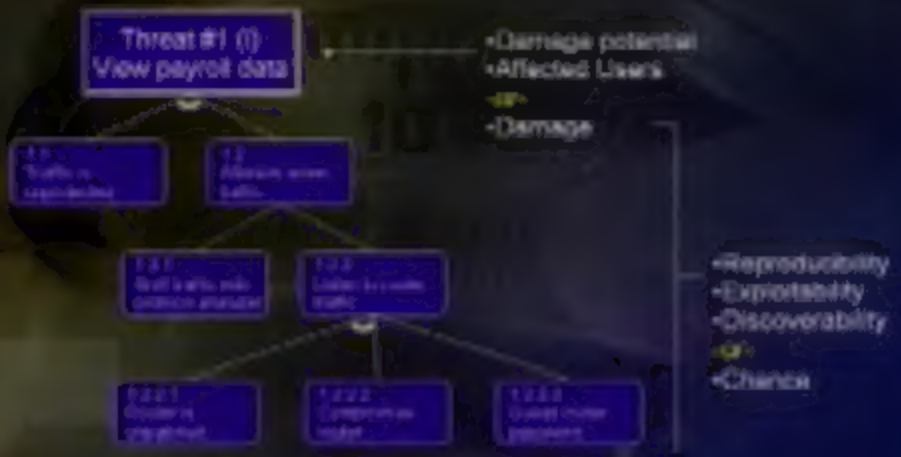
Portion of DFD

Information Disclosure Threat to Payroll Data



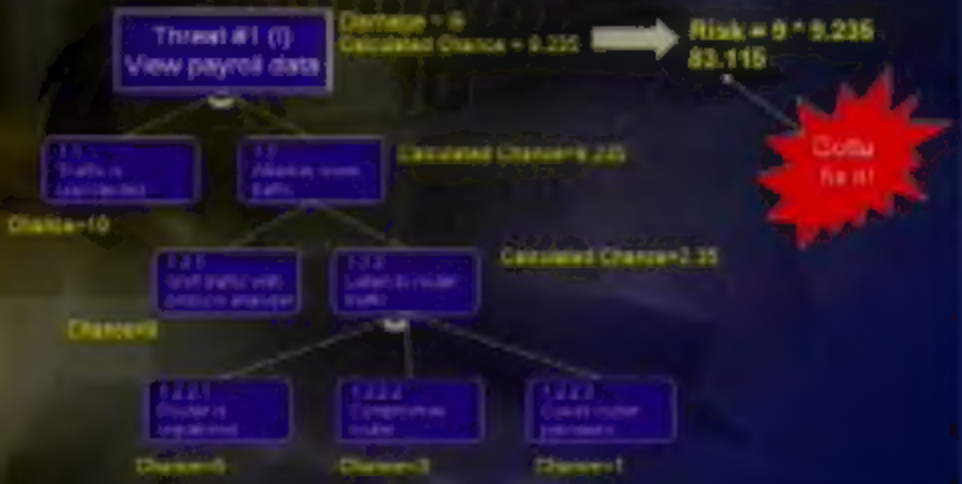
1.0 View payroll data (I)
- 1.1 Traffic is unprotected (AND)
- 1.2 Attacker views traffic
  - 1.2.1 Sniff traffic with protocol analyzer
  - 1.2.2 Listen to router traffic
    - 1.2.2.1 Router is unpatched (AND)
    - 1.2.2.2 Compromise router
    - 1.2.2.3 Guess router password

Applying Risk



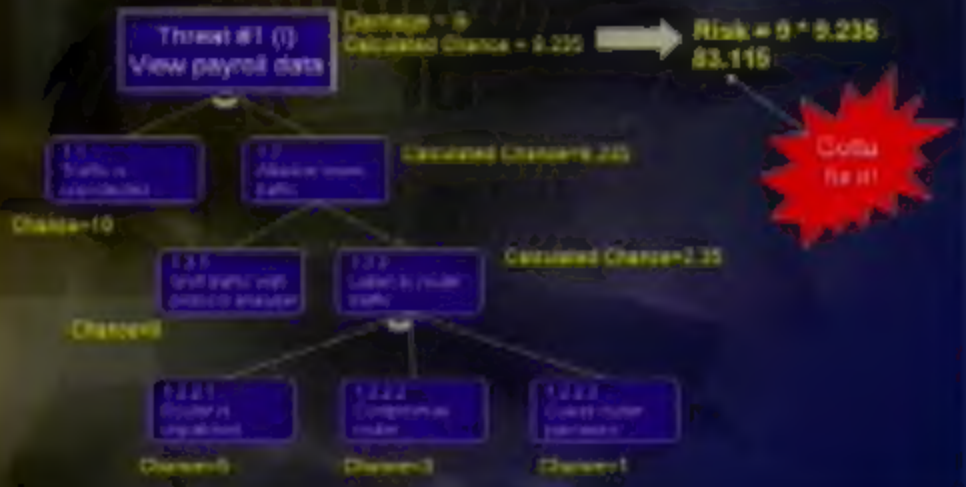
Applying Risk

Using combinatorics and Risk = Chance*Damage



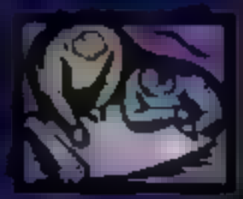
Applying Risk

Using combinatorics and Risk = Chance*Damage



Designing to a Threat Model

- Threat types and mitigation techniques
  - Spoofing
    - Authentication (public key, shared credentials, Kerberos)
  - Tampering
    - Authentication (passing, MAC), signing
  - Repudiation
    - Auditing, digital signatures, timestamps, trusted third parties
  - Information disclosure
    - Auditing, encryption
  - Denial of service
    - Filtering, quotas, authentication
  - Elevation of privilege
    - Run with constrained privileges



Threat Mitigation Techniques & Technologies


Threat Mitigation
Threat #1 (if
view payroll data
Look for high-level
AND clauses

Coding to a Threat Model

- Threat models help you determine the most 'dangerous' portions of the application
  - Prioritize security push efforts
  - Prioritize on-going code reviews
  - Help determine the defense mechanisms to use
- Determine data flow
  - All input is evil, until proven otherwise

Testing to a Threat Model

- Testers are part of the end-to-end process
- Each threat in the model must have a test plan
- The threat model helps drive testing concepts
- Allows for Whitehat and Blackhat testing
  - Testers should prove the mitigation works
  - Hackers should prove they don't work :-)

Testing to a Threat Model

- Mitigation techniques have blackhat testing technique
  - Spoofing
    - Authentication
      - Brute force creds, cred replay, downgrade to less secure authn, view creds on wire
    - Secure credential storage
      - Use information disclosure attacks
    - Authentication
      - Attempt authn bypass
    - SSL signing
      - Tamper and re-hash
      - Create invalid hash data

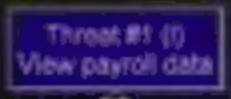
Testing to a Threat Model

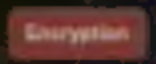
- Repudiation
  - Authn & Authz
    - See Spoofing and Tampering
  - Signing
    - See Tampering
  - Logging
    - Prevent auditing, spoof log entries (CR/LF)
  - Trusted third party
    - DoS the third party
- Info Disclosure
  - NOTE: Is there any PII data in the data?
  - Authorization
    - See Tampering
  - Encryption
    - View on-the-wire data
    - Kill process and scavenge for sensitive data
    - Failure leads to disclosure in error messages

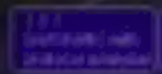
Testing Threat Mitigation

Functionally, is the traffic adequately protected?

Can you force the traffic to be unprotected?
Is the crypto weak?
Where is/are the keys) stored?
How are the keys exchanged?
Are the defense in depth methods ok?
Are there other conditions?







Threat Modeling Notes

- Scenario-driven
- Determine privilege to initiate data flow
  - Helps determine chance of attack
- Be wary of unauthenticated data flows
- All information disclosure threats are potentially privacy issues
- Any non-mitigated threat is a potential vulnerability
- All security features must mitigate one or more threats
- Work on the higher-risk items first


Microsoft